

What is claimed is:

1. A computer system, comprising:
a hard real-time operating system;
an application running under the hard real-time operating system; and
a security process running under the hard real-time operating system;
the security process is configured to
periodically, in hard real-time, check the integrity of the application and/or a data element used by the application and, if the integrity check of the application or the data element indicates that the application or data element has been tampered with, notify a user of the computer system and/or shut down at least part of the computer system or application, and
the security process includes a challenge handler that is configured to receive a challenge from an external monitor and provide a response thereto within a predetermined amount of time, wherein the external monitor is configured so that if the external monitor does not receive the response within a predetermined amount of time from sending the challenge, the external monitor notifies an administrator and/or shuts down at least part of the computer system or application.

2. In a computer system running a real-time operating system, a computer security method, comprising:

executing a security process under the real-time operating system, wherein the security process is configured to periodically, in hard real-time, check the integrity of an application and/or a data element used by the application and notify a system administrator and/or shut down the application if the integrity check of the application or the data element indicates that the application or data element has been tampered with;

sending a challenge to the security process or to a challenge handler that monitors the integrity of the security process; and

notifying an administrator if a response to the challenge is not received within a predetermined amount of time.

3. A computer system, comprising:

a dual-kernel operating system comprising a real-time kernel and a non-real-time kernel;

a first real-time thread running under the real-time kernel, the first real-time thread being configured to monitor the integrity of an application running under the non-real-time kernel;

a second real-time thread running under the real-time kernel, the second real-time thread being configured to monitor integrity of the first real-time thread; and

a security process running under the non-real-time kernel, the security process being configured to check the integrity of the first real-time thread and/or the second real-time thread.